Analyzing Security Solutions in Cloud Computing

Shashi Chhikara
Department of IT
ASET, Amity University

Iti Raghav
Department of IT
ASET, Amity University

Nitasha Hasteer
Acting Head,Department of IT
ASET, Amity University

ABSTRACT
In spite of the potential advantages of cloud computing, security is a major barrier to the adoption of cloud services for organizations, which forms the reasons for them not moving into the cloud. This paper provides a brief introduction to the cloud computing platforms and services it provides and we intend to discuss some of the key security issues that are associated with the cloud computing and analyze the possible security solutions.

General Terms
Cloud computing, security issues and threats

Keywords
Infrastructure as a service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Virtual Machine (VM), SOAP (Simple Object Access Protocol).

1. INTRODUCTION
The main idea behind cloud computing is not a new one. John McCarthy in the 1960s already envisioned that computing facilities will be provided to the general public like a utility[10].Cloud computing is a large-scale distributed computing paradigm [1]. It is a collection of sources in order to enable resource sharing in terms of scalability, managed computing services that are delivered on demand over the network NIST (National Institute of Standards and Technology) defines cloud computing as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of computing resources which can provisioned and released with nominal management effort or minimal service provider interaction [2]. This model promotes availability and is composed of three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS); the four deployment models are private cloud, community cloud, public cloud and hybrid cloud.

1.1 Cloud Computing characteristics
1.1.1 On demand Self Service
It refers to the service provided by various vendors that enables the provision of cloud resources on demand and whenever they are required.

1.1.2 Broad Network Access
Capabilities that are available over the network and accessed through standard mechanisms that promote use of heterogeneous thin or thick client platforms.

1.1.3 Resource Pooling
The service provider's computing resources are pooled together in order to serve multiple consumers, with different physical and virtual resources by dynamically assigning and reassigning these resources according to consumer demand.

1.1.4 Rapid Elasticity
Capabilities can be elastically provisioned and released depending on the requirement.

1.1.5 Measured Services
Cloud systems automatically control and optimize resource use by providing a metering capability at some level of abstraction according to the type of service.

1.2 Cloud Architecture
The general architecture of a cloud platform is also called cloud stack [3]. Built upon hardware facilities (usually supported by modern data centers), cloud services may be offered in various forms from the bottom layer to the top layer. In the cloud stack, each layer represents one service model. Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, where resources are accumulated and managed physically or virtually (e.g. Amazon EC2), and various services are delivered in forms of storage (e.g. GoogleFS), network (e.g. Openflow), or computational capability (e.g., Hadoop MapReduce). The middle layer delivers Platform-as-a-Service (PaaS), in which services are provided as an environment for the programmers or software execution (e.g., Google App Engine). Software as a Service (SaaS) locates in the top layer, in which a cloud provider further confines client flexibility by merely offering software application as a service. Apart from it, the cloud provider maintains a suite of management tools and facilities (e.g., Service life-cycle management, metering and billing) in order to manage a large cloud system.

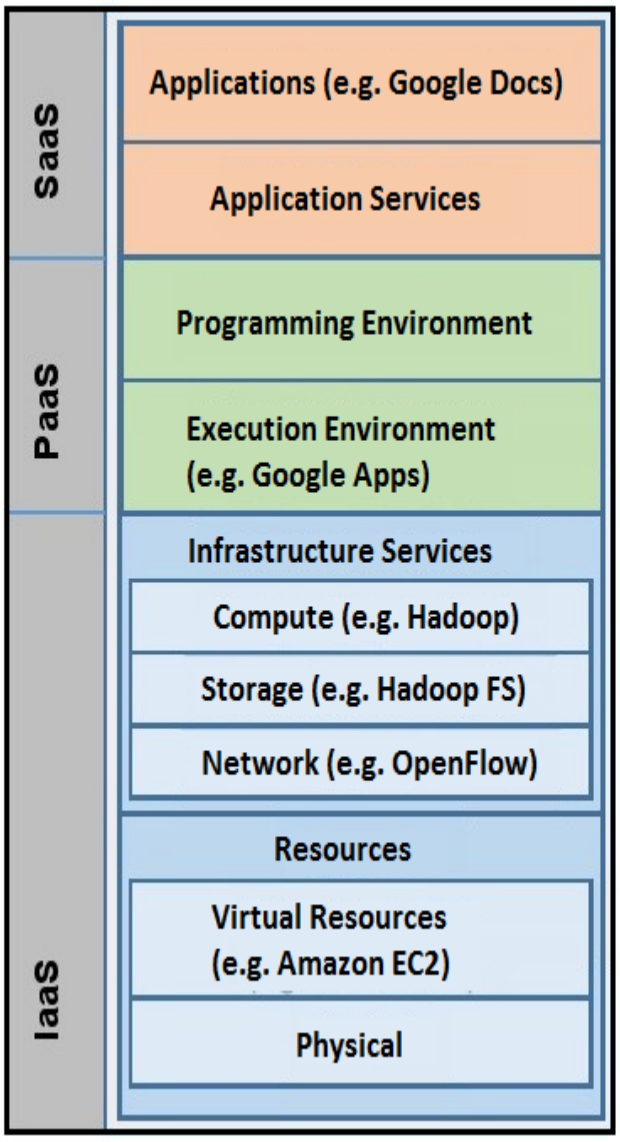

Fig. 1: Architecture of Cloud Computing

2. CLOUD COMPUTING SECURITY THREATS

2.1 Top Seven Cloud Security Threats

The top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are[4]:

2.1.1 Misuse And Vicious Use Of Cloud Computing

Misuse and vicious use of cloud computing is one of the main threat detected by the CSA. An easy to understand example of this is the use of bonnets to spread spam and malware. Malicious users can access a public cloud, for instance, find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.
Some remedies to minimize this threat:

- Apply strict initial registration and validation processes.
- Improved credit card fraud monitoring and coordination.
- Detailed introspection of customer network traffic.
- Supervising public blacklists for one's own network blocks.

2.1.2 Insecure Application Programming Interfaces

Because software interfaces or APIs are what customers use to interact with cloud services, those must have very secure access control, encryption, authentication and activity monitoring mechanisms - especially when third parties start to build on them.
Some remedies to minimize this threat:

- Examine the security model of cloud provider interfaces.
- Guarantees strong authentication and access controls are implemented in concert with encrypted transmission.
- Comprehend the dependency chain associated with the API.

2.1.3 Malicious Insiders

The CERT guide to cloud computing defines malicious insiders as "the current or the former employee, business partner who has or had authorized access to an structured system, data or network and intentionally misused and used in a manner affected the integrity, confidentiality and availability of the organization's information or information systems" [8]. Many service providers hide the way they hire people, how they grant the access to assets or how they supervise them. In this case, transparency is important to a secure cloud offering, along with compliance reporting and break notification.
Some remedies to minimize this threat:

- Impose supply chain management and conduct a comprehensive supplier assessment.
- Determine human resource requirements as part of legal contracts.
- Entail transparency into overall information security and management practices, as well as compliance reporting.
- Finding security breach notification processes.

2.1.4 Shared Technology Vulnerabilities

The parts on which the infrastructure is based were not designed for that. To ensure that customers don't pose danger on each other's "territory", monitoring and strong compartmentalization are required.
Some remedies to minimize this threat:

- Employ security best practices for installation/configuration.
- Scrutinize environment for unauthorized changes/activity.
- Support authentication and access control for administrative access and operations.
- Employ service level agreements for patching and vulnerability remediation.
- Perform vulnerability scanning and configuration audits.

2.1.5 Data Loss/Leakage

Data is always in danger of being lost or stolen. This is one of the zenith concerns for the organization, because they don't want to lose their reputation, but are also compelled by law to keep it safe.
Some remedies to minimize this threat:

- Employ strong API access control.
- Integrity of data is encrypted and protected.
- Examine data protection at both design and run time.
- Apply strong key generation, storage and management, and destruction practices.
- It is the duty of cloud providers to wipe persistent media before it is released into the pool.
- Contractually recognizes provider backup and retention strategies.

2.1.6 Account Service & Traffic Hijacking

Another consequences in which an attacker tries to attain access to your credentials, the attacker can eavesdrop on your activities and transactions, manipulate the data, return untrue

information, and channel into a new direction to illegitimate sites is by Account service and traffic hijacking
Some remedies to minimize this threat:

- Exclude the sharing of account credentials between users and services.
- Apply two-factor authentication techniques where possible.
- Use proactive monitoring to detect unauthorized activity.
- Understand security policies and SLAs of the cloud service providers..

2.1.7 Unknown Risk Profile

Important part of the priority list should be security. Code updates, exposure of profiles, security practices intrusion attempts – all points that should always be taken into account.
Some remedies to minimize this threat:

- Exposure of applicable logs and data.
- Partial/full disclosure of infrastructure details (*e.g.* patch levels, firewalls, etc.).
- Controlling and alerting on mandatory information.

2.2 Other Security Threats

Specific threats to security include[9][11]:

2.2.1 *Failures in Providers Security*

The Cloud service providers must monitor the hardware and the hypervisor on which data is stored and applications are run and therefore their security is very vital while designing cloud.

2.2.2 *Attacks by another customer*

If the barriers between customers collapsed, one customer can access another customer's data or interfere with their applications.

2.2.3 *Availability and reliability issues*

The cloud is only usable via the internet so internet reliability and availability is essential.

2.2.4 *Legal and Regulatory issues*

The virtual nature of cloud computing raises many legal and regulatory issues regarding the data exported outside the jurisdiction.

2.2.5 *Perimeter security model broken*

Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. The cloud is definitely beyond the perimeter of enterprise control but it will now store critical data and applications.

2.2.6 *Integrating Provider and Customer Security Systems*

Cloud providers should integrate with existing systems or the bad old days of manual provisioning and uncoordinated response will return.

2.2.7 Data Segregation

Generally, Data in the cloud is in a shared environment among with data of other customers. The encryption cannot be assumed as an only solution for all the data segregation problems. In some conditions, customers does not want to encrypt data because encryption accident can destroy or corrupt the data.

2.2.8 *Wrapping Attack*

A renowned type of attacks on protocols using XML Signature for authentication or integrity protection is wrapping attack. This applies to Web Services and therefore also for Cloud Computing [8].

2.2.9 Flooding Attack

Whenever a server is congested or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself.

Table 1: Security solutions and problems which have been proposed by ArmMichaelHalton[12]:

Security Threat	Solution
Cross scripting, SQL injections	A security oriented framework that applies best programming practices.
TCP/IP and/or the operating systems vulnerabilities	Up-date applications in a timely manner, Deactivate unused services and manage control rights.
Authentication: RIP attacks, IP spoofing, , ARP poisoning	Use encrypted protocols, control rights to access ARP tables.
Tampering and loss of data	Encrypt the data
Physical Access	Control the rights and log the actions

3. EXISTING SOLUTIONS FOR SECURITY THREATS

There are some existing solutions for the security threats:

3.1 Client Based Privacy Manager

Client based privacy manager helps to minimize the risk of data leakage and loss of privacy of the sensitive data processed in the cloud and provides additional privacy related benefits [5]. Figure 2 shows the architecture of the privacy manager. The main features of the privacy manager are:

- **Obfuscations:** This feature can automatically obfuscate some or all of the fields in a data structure before it is sent off to the cloud for processing, and converts the output from the cloud back into deobfuscated form. The obfuscation and deobfuscation is done with the help of a key which is selected by the user and not revealed to cloud service providers.
- **Preference Setting:** It allows users to set their priorities about handling of personal data that is stored in an unobfuscated form inside the cloud. This feature permits the user to take maximum charge over the usage of his data.
- **Data Access:** The Privacy Manager holds a module that permits users to access personal information in the cloud, in order to see what is being possessed about for , and to check its correctness. This is an auditing mechanism

which will identify privacy violations once they have occurred.

- **Feedback:** It manages and portraits feedback to the user in respect of the usage of his personal information, including notification of data used in the cloud. This module could supervise personal data that is transferred from the platform.
- **Personae:** This feature permits the user to choose between numerous personae when dealing with cloud services.

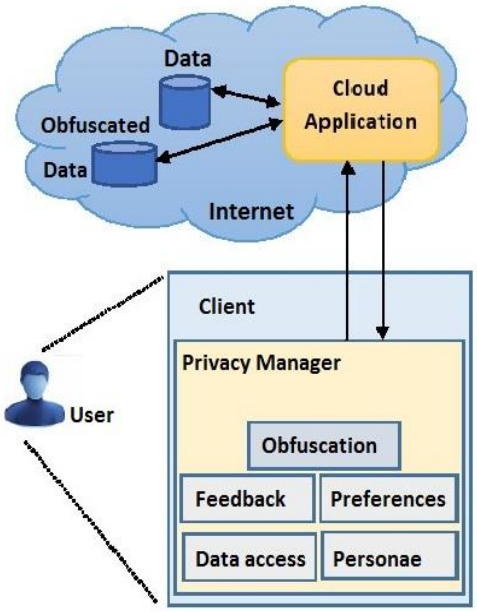

Fig.2: Architecture of Privacy Manager [5]

3.2 Mirage Image Management System

The security and integrity of VM images are the foundation for the overall security of the cloud since many of them are designed to be shared by various and frequently unrelated users [6]. This system caters the issues related to security management of the virtual-machine images that encapsulate each application of the cloud.

Mirage Image Management System contains 4 major parts:

- **Access Control:** This framework controls the sharing of VM images. Each image in the repository has a distinct owner, who can share images with trusted parties by permitting access permissions.
- **Image Transformation by Running Filters:** Filters abolish unwanted information from images at publishes and retrieval time. Filters at publish time can discard or conceal sensitive information from the publisher's original image. Filters at retrieval time filters may be mentioned by the publisher or the retriever.
- **Provenance Tracking:** This process that tracks the derivation history of an image.
- **Image maintenance:** Depository maintenance services, such as periodic virus scanning, that identify and correct vulnerabilities discovered after images are published.

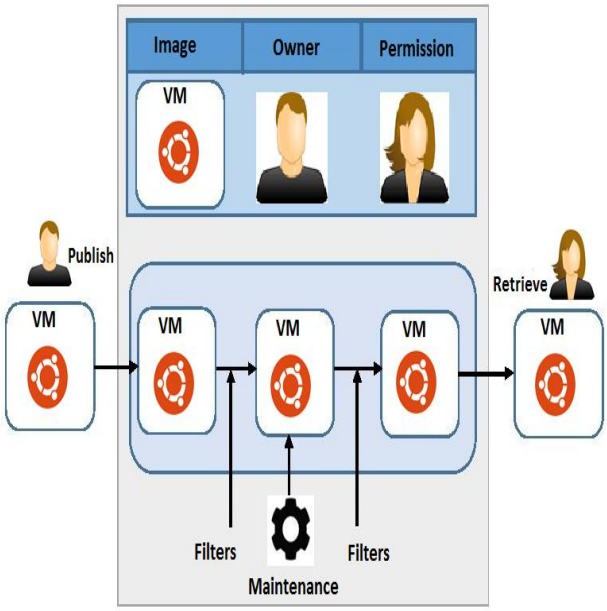

Fig 3: Architecture of Mirage Image Management System

Advantages: Filters mitigate the danger in a systematic way. The system stores all the revisions which permit the user to go back to the previous version. The default access permission of an image is private in order to provide access to the owner and system administrator can access the image and hence untrusted parties cannot access the image.

Disadvantages: Large performance overheads, in terms of space and time. It is not possible for filters to be 100% accurate and therefore the system does not remove risk. Virus scanning does not promise to find all malware in an image.

3.3 Wrapping Attack Problem and Solution

When a user makes a request from his VM via the browser, the request is first directed to the web server. A SOAP (Simple Object Access Protocol) message is generated that contains the structural information that will be exchanged between the browser and server during the message passing. The SOAP header should contain all the necessary information for the destination after computation is done. For a wrapping attack, the opponent does its trick during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message and signature value is duplicated and sent to the server as a valid user. The server checks the authentication and integrity and as a result, the adversary is able to intrude in the cloud and can run malicious code.

Possible Solution

Since an adversary can intrude in the TLS layer; to increase the security during the message passing from the web server to a web browser by using the SOAP message. As the signature value is appended, we can add a redundant bit (STAMP bit) with the SOAP header. When the message is interfered when this bit will be toggled. The STAMP bit is checked first and if it is found toggled, then a new signature value is produced in the browser end and the new value sent back to the server as recorded to modify the authenticity checking.

Advantage:

- It is advantageous for many applications:business process scenario, single sign on.

Disadvantages:

- Lack of processing applications.
- It doesn't check if has the same values.

3.4 Flooding Attack Problem and Solution

Whenever a server is congested or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself [8]. When an adversary has achieved the authorization making a request to the cloud, then he/she can simply create false data and pose these requests to the cloud server. As a non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to large scale. As a result, legitimate services can starve the server will offload its services to another server. Repeating the adversary is successful in engaging the whole cloud system by interrupting the normal processing of one server, in particular flooding system.

Possible solution

The approach is to put in order all the servers in the cloud system as a group of servers. Each of the servers will be designated for a particular type of job. All the servers in the group will have internal communication among themselves via message passing. Therefore when a server is overloaded, a new server will be implemented in the fleet. A hypervisor can also be utilized for the scheduling among these fleets, finding the genuineness of the requests and preventing the fleets from being overloaded with bogus requests from an adversary.

Advantages

- Whenever a server is congested or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself.
- Requests are executed more efficiently and rapidly.

4. CONCLUSION AND FUTURE WORK

There is a lot of personal and private information and potentially secure data that people store on their computers, and this information is sent to the cloud.This makes security in the cloud a primary concern. This paper discussed the various security issues of cloud computing along with their models to overcome them. It also enlightens various advantages and disadvantages of the solutions that are widely available. Hence it also motivate to explore this area further inorder to overcome the problems that are faced by the cloud community.

5. REFERENCES

[1] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. Elhariri, Ahmed M. Yousof and Sahar A. Shehata. 2012. A Hierarchical Intrusion Detection System For Clouds: Design And Evaluation. International Journal on Cloud Computing: Services and Architecture.

[2] Peter Mell, and Tim Grance, 2009 "The NIST Definition of Cloud Computing," Version 15, National Institute of Standards and Technology (NIST)

[3] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm 2009."What's Inside the Cloud? An Architectural Map of the Cloud Landscape". Software Engineering Challenges of Cloud Computing. CLOUD'09. ICSE Workshop in 2009.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[5] Miranda Mowbray, Siani Pearson. 2009."A Client-Based Privacy Manager for Cloud Computing**:"** COMSWARE '09**:** Proceedings of the Fourth International ICST Conference on COMmunication System software and middleware

[6] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. 2009."Managing security of virtual machine images in a cloud environment*." CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security.*

[7] D. Cappelli, A. Moore, and R. Trzeciak, 2012. "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)", ser. SEI Series in Software Engineering. Addison-Wesley, Professional.

[8] B.Meena, Krishnaveer Abhishek Challa. 2012."Cloud Computing Security Issues with Possible Solutions."in IJCST

[9] Steve Hanna. A security analysis of Cloud Computing. Cloud Computing Journal. DOI = http://cloudcomputing.sys-con.com/node/1203943

[10] Guide to Cloud Computing: Principles and Practice By Richard Hill, Laurie. Hirsch, Peter. Lake, Siavash Moshiri, Page 16-18, 1996.

[11] Vahid Ashktorab, Seyed Reza Taghizadeh, 2012. "Security Threats and Countermeasures in Cloud Computing" in IJAIEM.

[12] David Munoz Sanchez, Comparison between security solutions in Cloud and Grid Computing. Aalto University, T-110.5290 Seminar on Network Security Fall 2010.